IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for providing security for a computer network, comprising:

automatically generating content for a computer~~, wherein the computer is~~ associated with the network;

creating on the computer a deception environment comprising a fully functional operating system and the automatically generated content;

determining automatically based on a preconfigured policy not specific to any user whether a user should be routed to the deception environment; ~~generated content;~~ and

routing the user to the deception environment ~~generated content~~ if it is determined that the user should be routed to the ~~generated content.~~; deception environment;

wherein the quantity and substance of the generated content are such that the deception environment would present to an intruder a credible version of a system such as the intruder would expect to see upon gaining unauthorized access to the computer.

2. (Original) The method of claim 1, further comprising monitoring the activities of the user with respect to the computer.

3. (Currently amended) The method of claim 2, further comprising automatically preventing the user from accessing ~~files associated with said monitoring.~~ a file which if accessed would reveal to the user that an activity of the user is being monitored.

4. (Original) The method of claim 1 further comprising storing the packets sent by the user.

5. (Original) The method of claim 1 further comprising logging information concerning the files to which the user requests access.

6. (Original) The method of claim 1 further comprising preventing the user from accessing content within the computer other than the generated content.

7. (Original) The method of claim 1 further comprising screening a request by the user to access a file to determine if access is permitted.

8. (Original) The method of claim 7 further comprising permitting access to a requested file if it is determined that access to the requested file is permitted.

9. (Original) The method of claim 7 further comprising providing an indication that a requested file does not exist if it is determined that access is not permitted.

10. (Original) The method of claim 1 further comprising generating additional content subsequent to the step of generating content.

11. (Original) The method of claim 10 further comprising adding the additional content to the previously-generated content.

12. (Currently Amended) The method of claim 1 wherein the step of routing comprises using network address translation to route to the deception environment ~~generated content~~ any user that requests to access an unauthorized service.

13. (Original) The method of claim 12 wherein the unauthorized service is telnet.

14. (Original) The method of claim 1 further comprising receiving an indication that the user is no longer connected to the computer.

15. (Original) The method of claim 14 further comprising determining whether to retain changes in the files of the computer that resulted from the user's activities.

16. (Currently Amended) The method of claim 15 further comprising resetting the computer to restore the computer and the generated content to the condition they were in prior to the user being routed to the deception environment ~~generated content~~ if it is determined the changes should not be retained.

17. (Original) The method of claim 16 further comprising updating the generated content by generating additional content that appears to have been created during the time period during which the user was connected to the computer.

18 – 29. (Canceled)

30. (Currently Amended) A system for providing security for a computer network, comprising:

a computer configured to:

automatically generate content for the computer, wherein the computer is associated with the network; and

create on the computer a deception environment comprising a fully functional operating system and the automatically generated content; and

a network device configured to:

determine automatically based on a preconfigured policy not specific to any user whether a user should be routed to the deception environment; and

route the user to the deception environment if it is determined that the user should be routed to the deception environment;

wherein the quantity and substance of the generated content are such that the deception environment would present to an intruder a credible version of a system such as the intruder would expect to see upon gaining unauthorized access to the computer.

~~a computer configured to generate content for the computer, wherein the computer is associated with the network; and~~

~~a network device configured to determine whether a user should be routed to the generated content and to route the user to the generated content if it is determined that the user should be routed to the generated content.~~

31. (Original) The system of claim 30, wherein the network device is a firewall.

32. (Currently Amended) A computer program product for providing security for a computer network, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

automatically generating content for a computer~~, wherein the computer is~~ associated with the network;

creating on the computer a deception environment comprising a fully functional operating system and the automatically generated content;

determining automatically based on a preconfigured policy not specific to any user whether a user should be routed to the deception environment; ~~generated content;~~ and

routing the user to the deception environment ~~generated content~~ if it is determined that the user should be routed to the ~~generated content.;~~ deception environment;

wherein the quantity and substance of the generated content are such that the deception environment would present to an intruder a credible version of a system such as the intruder would expect to see upon gaining unauthorized access to the computer.

33. (New) The method of claim 1, wherein creating the deception environment comprises:

establishing a cage within a trap host system;

copying a trap host system operating system to the cage; and

copying a trap host system file system to the cage;

wherein the trap host file system comprises the automatically generated content.